STATE OF VERMONT
Agency of Human Services (AHS)

Security Assessment	REVISION HISTORY:	Chapter/Number 5.08
	EFFECTIVE DATE: 10/23/08	Attachments/Related Documents:

Authorizing Signature: Cynthia D. LaWare Date Signed: 10/23/08
Cynthia D. LaWare, Secretary, Agency of Human Services

PURPOSE:

To ensure the development, dissemination, and periodic review/update of documented security assessment policies and procedures.

BACKGROUND and REFERENCES:

National Institute of Standards and Technology (NIST) Special Publication 800-53, *Information Security*

NIST Special Publication 800-30, *Risk Management,* (NIST Special Publications available at http://csrc.nist.gov/publications/PubsSPs.html)

DEFINITIONS:

Security Controls- The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information (as defined in NIST SP 800-53, Appendix B)

Legacy Systems- applications that have exceeded a normal lifecycle and are usually supported by dated technologies.

SCOPE:

This document applies to all Agency Departments, Divisions and Offices hereafter referred to jointly as "department". This document also applies to contractors, business associates, and other users of departmental information systems.

STANDARDS:

The Agency shall conduct an assessment of the risks and security controls in designated information systems at least every two years to determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

The AHS CIO and AHS Information Systems Security Director shall work with departments' IT Managers to identify and prioritize AHS information systems and schedule security assessments.

As a result of this policy, AHS shall develop procedures to establish and maintain the following capabilities:

- Ensure the management, operational, and technical controls in each information system contained in the inventory of information systems are assessed with a frequency depending on risk.
- Authorize all connections (interfaces) from the information system to other information systems through the use of system connection agreements and monitor/control the system connections on an ongoing basis.
- Conduct an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- Develop and update a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.
- Monitor the security controls in the information system on an ongoing basis.
- Establish criteria for designating an information system to be assessed.

COMPLIANCE:

It is the responsibility of the individual departments IT Managers and the AHS CIO to ensure dissemination and review of this policy to all employees within their organizations and other associates, as appropriate.

AHS departments with legacy systems or other extenuating circumstances must apply in writing to the AHS CIO for exceptions to this policy per information system.

ENFORCEMENT:

The Office of the Secretary may initiate reviews, assessments or other means to ensure that policies, guidelines or standards are being followed.